**BURSOR & FISHER, P.A.**
L. Timothy Fisher (State Bar No. 191626)
Stefan Bogdanovich (State Bar No. 324525)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
sbogdanovich@bursor.com

*Attorneys for Plaintiffs*

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA—EASTERN DIVSION**

ISIAH SHEPPARD, HILSCIO RIVERA, HELENE LAUZIER-MEYER, and BERNABE BENITEZ, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

FANTASIA TRADING LLC, d/b/a EUFY,

Defendant.

Case No. 5:23-cv-2407

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs Isiah Sheppard, Hilscio Rivera, Helene Lauzier-Meyer, and Bernabe Benitez ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Defendant Fantasia Trading LLC, d/b/a Eufy ("Defendant" or "Eufy") for violations of Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.* The following allegations are based on their counsel's investigation and upon information and belief, except for allegations concerning Plaintiffs themselves, which are based on personal knowledge.

## NATURE OF THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing, and using their and other similarly situated individuals' biometric identifiers and biometric information (referred collectively at times as "biometrics") without first obtaining informed written consent and failing to provide the requisite data retention and destruction schedule, in direct violation of BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identify theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual's biometrics unless it informs that person in writing that biometric identifiers or information will be collected or stored. *See* 740 ILCS 14/15(b).

4. Likewise, BIPA also requires that entities collecting biometrics must publish and make publicly available written retention schedules and guidelines for permanently destroying biometrics collected. *See* 740 ILCS 14/15(a).

5. Defendant advertises a Person Detection feature as part of its home security systems. Defendant's home security systems incorporate artificial intelligence ("AI") monitoring dubbed either "Local AI" or "BionicMind" to scan faces and bodies while collecting and storing these biometrics. These technologies "can differentiate between family members and strangers" to "[r]educe [u]nnecessary [a]lerts."[1]

6. In direct violation of each of the foregoing provisions of §§ 15(b) and 15(a) of BIPA, Defendant collected, stored, and used—without providing notice, obtaining informed written consent and without publishing a data retention schedule—the biometric identifiers and biometric information of delivery drivers making deliveries to homes using Defendant's home security system.

7. BIPA confers on Plaintiffs, and all those similarly situated Illinois residents who make home deliveries, the right to know of such risks, which are inherently presented by the collection and storage of their biometrics. Plaintiffs also have a right to know how long such risks will persist while their biometrics are stored and used by Eufy's AI, which, once collected and stored, scans biometrics to create mechanical measurements necessary for identifying and differentiating specific shapes, objects and people.

8. This is particularly concerning because other home security companies like Google Nest and Wyze do not allow their cameras and doorbells with facial recognition capabilities to be used in Illinois.[2]

---

[1] Eufy, *eufyCam 3*, available https://us.eufy.com/pages/security-eufycam3 (last accessed Oct. 24, 2023).

[2] Google Store, *Nest Aware*, available at https://store.google.com/us/product/nest_aware?hl=en-US&pli=1 (last accessed Oct. 18, 2023); Wyze, *How do I set up Friendly Faces?* (July 21, 2023), available at https://support.wyze.com/hc/en-us/articles/5876322908315-How-do-I-set-up-Friendly-Faces- (last accessed Oct. 18, 2023).

9. Plaintiffs bring this action to prevent Defendant from further violating the privacy rights of Illinois delivery drivers and to recover statutory damages for Defendant's unauthorized collection, storage, and use of their biometrics in violation of BIPA.

## PARTIES

10. Plaintiff Isiah Sheppard is a resident of Illinois. Plaintiff Sheppard works as an Uber Eats and DoorDash delivery driver who makes deliveries to customers' homes. As part of Plaintiff Sheppard's regular deliveries process, he walks to the front door of the customer's residence to make the delivery. On multiple deliveries, scans of Plaintiff Sheppard's face and/or hands were captured by Defendant's security system.

11. Plaintiff Hilscio Rivera is a resident of Illinois. Plaintiff Rivera works as an Amazon, DoorDash, Postmates, Dispatch, Veho, AxleHire and Roadie delivery driver who makes deliveries to customers' homes. As part of Plaintiff Rivera's regular delivery process, Plaintiff Rivera walks to the front door of the customer's residence to make the delivery. On multiple deliveries, scans of Plaintiff Rivera's face and/or hands were captured by Defendant's security system.

12. Plaintiff Helene Lauzier-Meyer is a resident of Illinois. Plaintiff Lauzier-Meyer works as a DoorDash and Spark delivery driver who makes deliveries to customers' homes. As part of Plaintiff Lauzier-Meyer's regular deliveries process, she walks to the front door of the customer's residence to make the delivery. On multiple occasions, scans of Plaintiff Lauzier-Meyer's face and/or hands were captured by Defendant's security system.

13. Plaintiff Bernabe Benitez is a resident of Illinois. Plaintiff Benitez works as an UberEats delivery driver who makes deliveries to customers' homes. As part of Plaintiff Benitez's regular deliveries process, he walks to the front door of the customer's residence to make the delivery. On multiple occasions, scans of Plaintiff Benitez's face and/or hands were captured by Defendant's security system.

14. Defendant Fantasia Trading LLC is a Delaware corporation with its principal place of business in Ontario, California. Fantasia Trading LLC is the parent company of Anker Innovations and Eufy.

15. Eufy is a home security technology company that offers security cameras supported by high quality video and artificial intelligence ("AI") monitoring.

## JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs, and at least one class member is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business in this district, in Ontario, California.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is at home in this District.

## FACTUAL ALLEGATIONS

### I. Eufy's Home Security System, Local AI and BionicMind AI.

19. Eufy is an emerging leader in home security systems. However, Eufy "isn't like your traditional alarm company. It's a tech company first[.]"[3]

20. To that end, Eufy sells 36 different security camera models, each equipped with on-device AI monitoring capabilities.[4] These cameras include

[3] Aliza Vigderman & Gabe Turner, *Eufy Security System Review and Cost*, Security.org (Oct. 12, 2023) *available* https://www.security.org/home-security-systems/eufy/ (last accessed Oct. 18, 2023).

[4] Eufy, *AI Features for eufySecurity Devices*, available https://support.eufy.com/s/article/AI-Features-for-eufySecurity-Devices (last accessed Oct. 18, 2023).

multiple models of doorbell cameras, exterior mounted and floodlight cameras, and a series of base stations.[5]

21. Eufy's AI technology is categorized as either "Local AI" or "BionicMind AI." Together, they offer homeowners several different detection features depending on the user's subscription and base station.

22. "Local AI" (Eufy's on-device AI mechanism) uses an "embedded AI chip" built into the cameras which provides "local, safe, and intelligent detection."[6]

23. The "BionicMind AI" system "has the ability to recognize similar faces, body shapes/positions, different objects, and even human behavior with its machine self-learning system."[7] The system conducts this analysis "locally on the base station"[8] and is added to an already operating Eufy system by incorporating the proper base station.

24. Eufy's intelligent detection arises through six unique features: (1) a human detection feature where the system tries "to detect objects similar to the human shape and filter out other objects like cars and animals for motion alerts;" (2) facial detection where the system tries to "detect and screen faces shown in the video image;" (3) human facial recognition where the system tries to "recognize faces in the video image and identify the person for [the homeowner];" (4) pet detection where the system tries "to detect pets which appear in the video image;" (5) crying detection where the system tries "to detect crying and will notify [the homeowner] if

---

[5] *Id.*

[6] *Id.*

[7] Jared Locke, *Eufy's Latest Edge Security System Features Self-Learning AI to Identify Family and Friends*, 9To5 Toys (Sep. 30, 2022) *available* https://9to5toys.com/2022/09/30/eufy-edge-security-system-launch/ (last accessed Oct. 23, 2023).

[8] *Id.*

necessary;" and (6) vehicle detection where the system "will catch up with the user's vehicle in the backyard or driveway."[9]

25. Generally, the kind of base station the homeowner uses impacts which version of Eufy's AI the homeowner can turn on. For example, the base level "Original HomeBase" allows all AI-incorporated cameras and battery-operated video doorbells to use the human detection and facial recognition features. The "HomeBase 3", alternatively, allows the homeowner to deploy each AI recognition feature. "HomeBase E" and "HomeBase 2" allow the homeowner to use just the Human Detection and Facial Recognition detection features.[10]

26. However, unlike the rest, Eufy's *wired* video doorbells allow the homeowner to use the human and facial detection features without needing a base station.[11]

27. Regardless of which camera is used, Eufy's Local AI system is remarkably accurate. As Eufy boasts, its on-camera AI human detection feature "accurately detect[s] humans and vehicles" 95% of the time.[12]

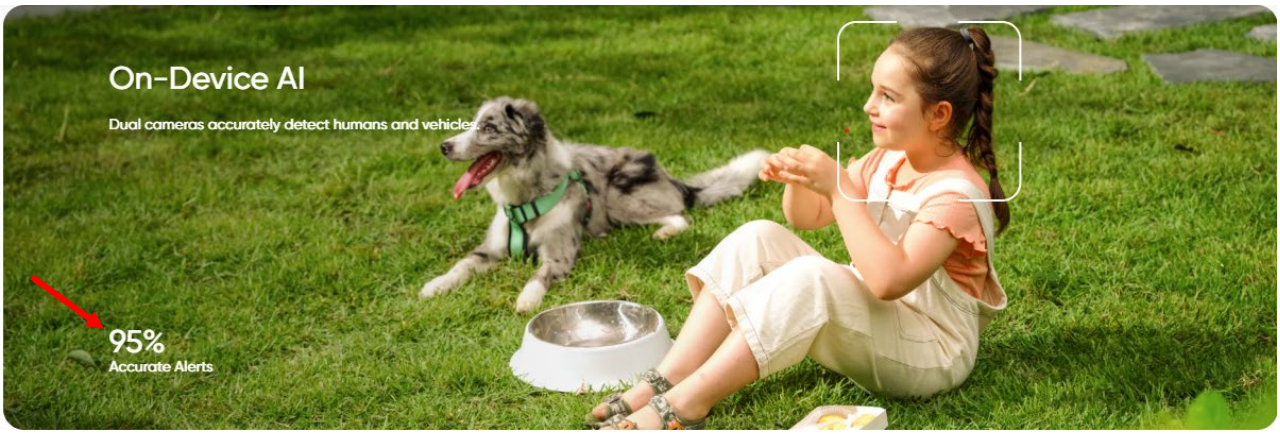
---

[9] Eufy, *supra* note 4.

[10] *Id.*

[11] *Id.*

[12] Eufy, *SoloCam S340*, available https://www.eufy.com/solocam-s340?utm_source=google&utm_medium=search&utm_content=alwayson&utm_campaign=us_security_edge_conversion_search_eufycam_purchase_ost_M3_bb&utm_term=19626718763_144313519606_676641948951&gclid=CjwKCAjwvrOpBhBdEiwAR58-3NdpFPlGlnThHvpGuSIhMB31i0N0GkYya92NvW0IIXAjSnobXtGefBoCVVoQAvD_BwE (last accessed Oct. 19, 2023).




28. Likewise, users can enhance their system's AI capabilities by adding Eufy's BionicMind AI-equipped base stations to their security systems.[13] Eufy's BionicMind AI system, which can be added simply by connecting a new base station,[14] "uses self-learning algorithms after every facial and body shape scan to improve recognition accuracy to more than 99.9% over time—no matter what [the subject is] wearing and how [the subject] approach[es] the camera."[15]

[13] *See* Jennifer Pattison Tuohy, *Eufy's Impressive New Smart Cameras Use AI to Identify You and Your Pets*, The Verge (Sep. 30, 2022) *available* https://shorturl.at/uNST4 (last accessed Oct. 20, 2023).

[14] *See Id.* ("HomeBase 3 has expandable local storage up to 16 TB, while adding the power of BionicMind for an accurate AI experience.")

[15] Eufy, *eufyCam 3*, *available* https://shorturl.at/crHKQ (last accessed Oct. 19, 2023).


29. Human detection, available for "Local AI" and "BionicMind AI" users, "detects and captures motion . . . for accurate object classification."[16] The technology "works in two steps[.]"[17] First, "[w]hen the camera detects motion in its field of view, the AI engine analyzes the figure to determine if it is a human being or not."[18] Second, "if the captured face meets the AI engine's analysis parameters, the AI engine will try to capture the face and then send a notification to the user."[19] This step allows the system to use the captured biometrics in two scenarios.

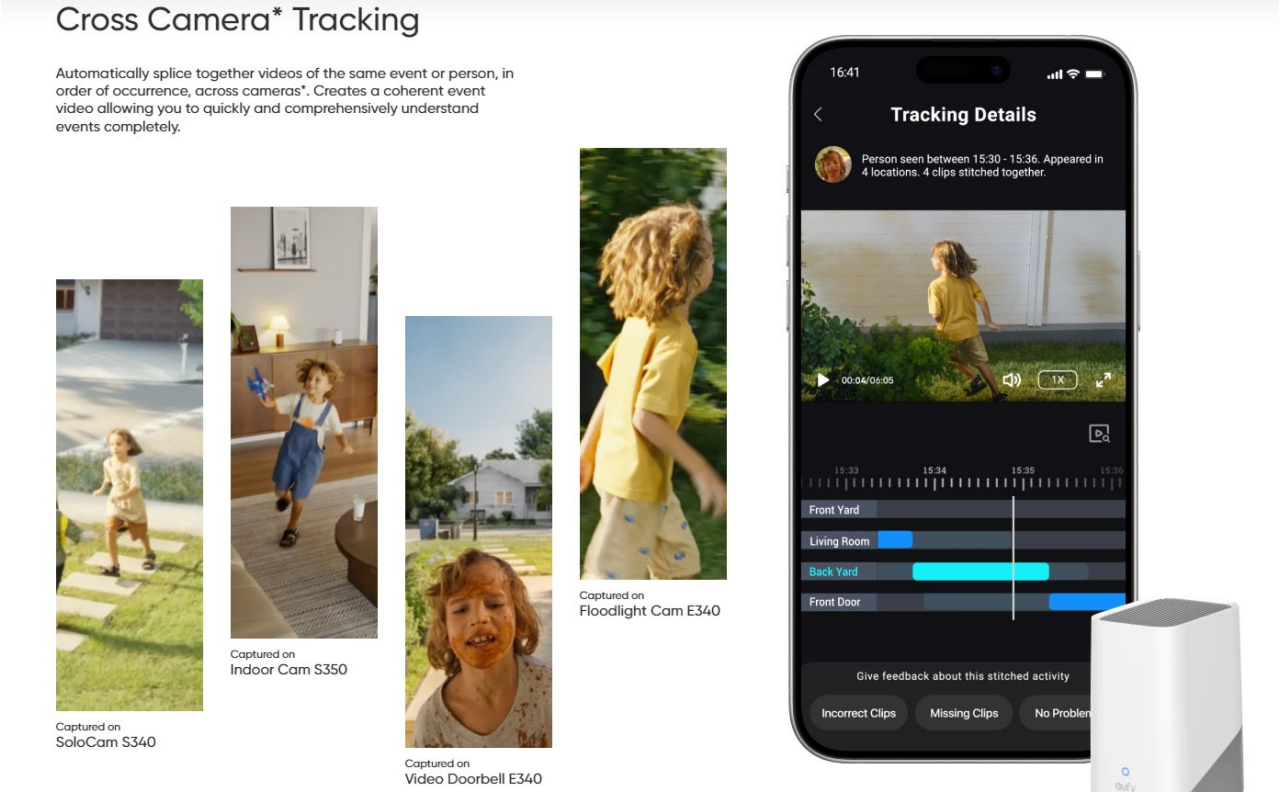
[16] Eufy, *How Does the Human Detection Technology Work?* available https://shorturl.at/hqr79 (last accessed Oct. 19, 2023).

[17] *Id.*

[18] *Id.*

[19] *Id.*


30. One such feature is "cross camera tracking" where, once stored with the proper base station connected, Eufy's system will "automatically compile shots **of the same event and person** and organize them chronologically into a single clip"[20] if an event occurs within the view of multiple cameras.

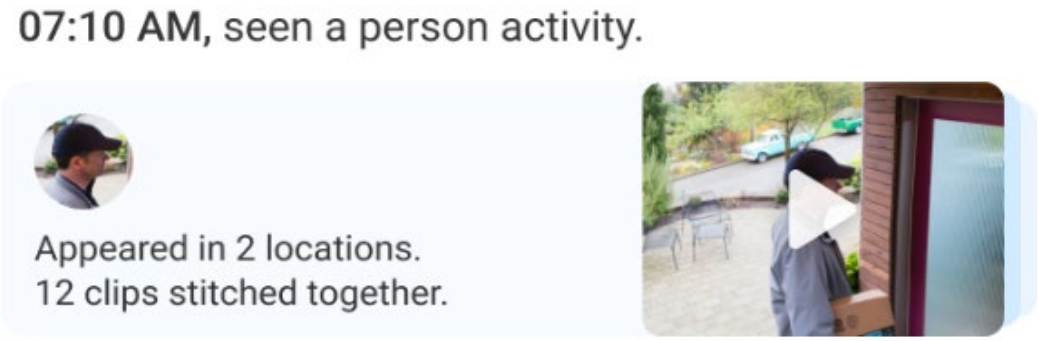



[20] Anthony Spadafora, *Eufy's New Security Cameras Use AI for Cross-Camera Tracking—Here's How it Works*, Yahoo! Finance (Sep. 26, 2023) *available*

31. As Eufy explains, "[w]hen the same individual appears across multiple cameras within a specified timeframe, the system automatically locates and merges these footage [sic] into a single video" so that the homeowner can "easily review the entire activity **of that specific individual** in a single video."[21]

32. To piece the footage together, the BionicMind base station "analyzes the video content and stitches it together in-real [sic]" time and, "[a]fter each camera has finished recording and saving videos to [the base station], [] re-analyzes the video content for splicing."[22] Cameras that are not compatible with BionicMind base stations cannot stitch images together in real time and, instead, analyze saved video after recording has ended.[23]

33. The homeowner then receives a notification alerting them that the device has either detected an already cataloged face like a friend or a new, unknown visitor like a delivery driver:

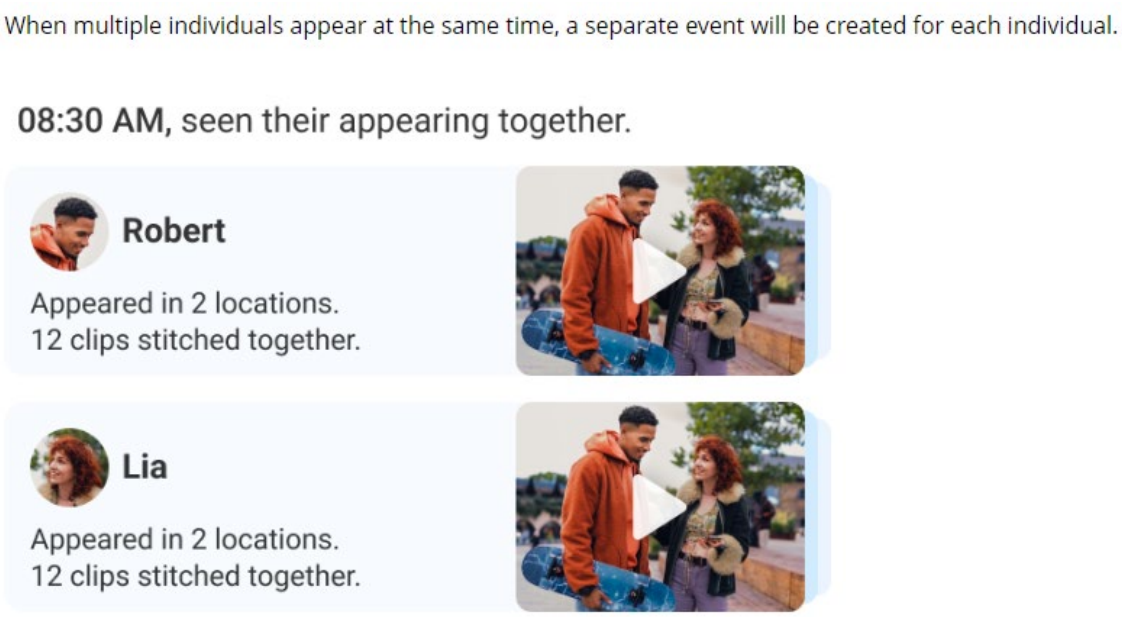



https://finance.yahoo.com/news/eufy-security-cameras-ai-cross-230048637.html. (emphasis added).

[21] Eufy Support, *Introducing the Cross-Camera Tracking Function in the Eufy Security App*, Eufy *available* https://support.eufy.com/s/article/Introducing-the-Cross-Camera-Tracking-Function-in-the-eufy-Security-App (last accessed Oct. 20, 2023) (emphasis added).

[22] *Id.*

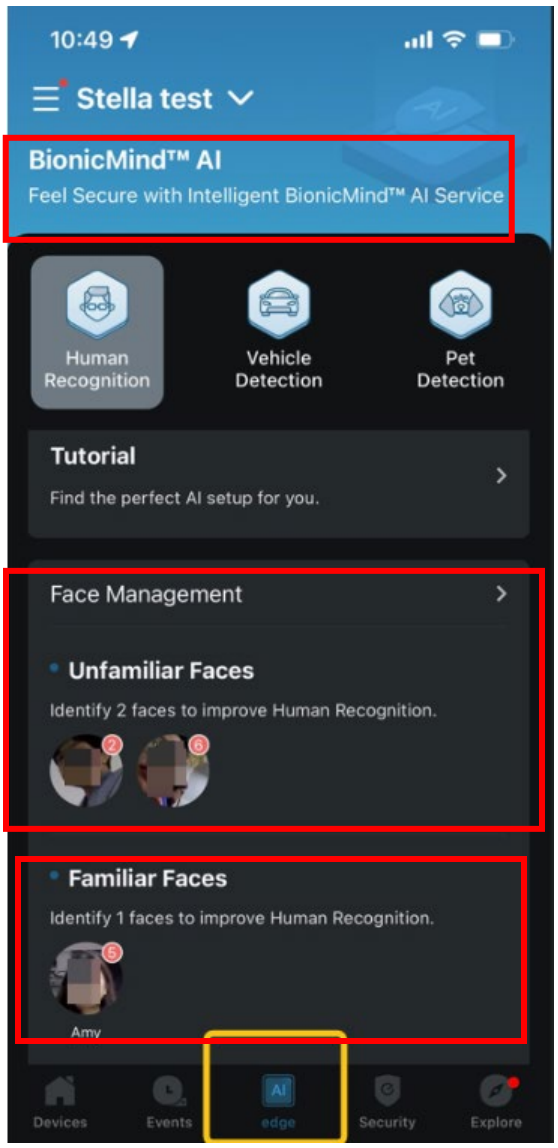
[23] *See Id.* ("Cameras that are compatible with HomeBase 3 storage, but not with HomeBase 3 BionicMind [] A.I., will only be able to use the Look-Back Tracking Function. . .").

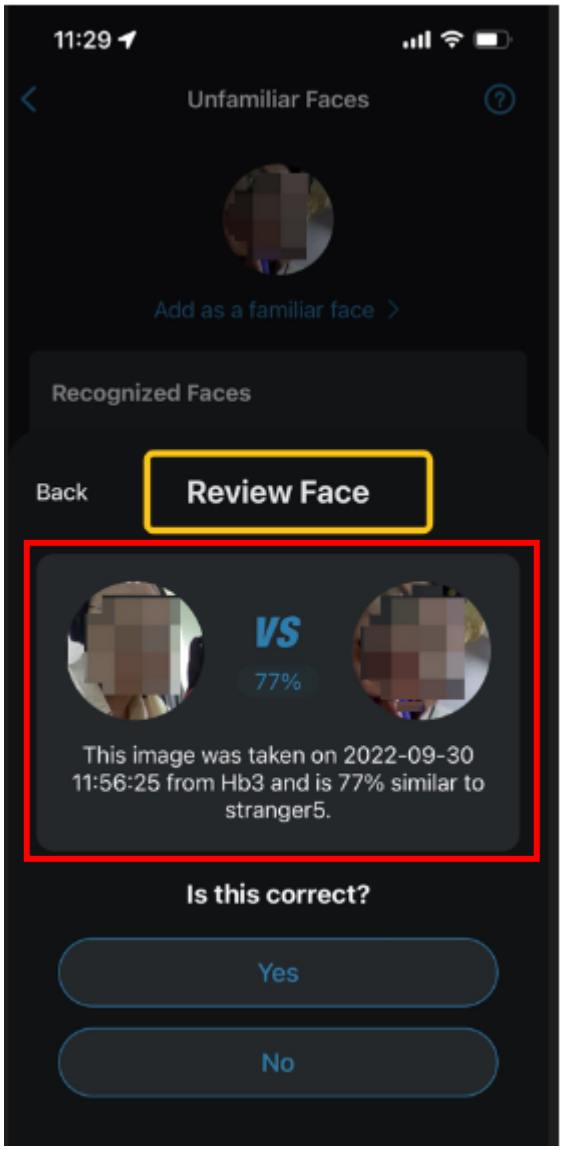



34. Eufy is capable of making these identifications by storing and analyzing biometric data so the AI can "keep learning the details of the characteristics of people, including different angles of the face and bodies" to "help the AI recognize a person more accurately and quickly."[24] That data is then accessible to the user via the EufySecurity App.[25]

[24] Eufy Support, *What is the self-learning AI in the HomeBase 3?* Eufy (Dec. 1, 2022) *available* https://support.myeufy.com.au/support/solutions/articles/73000597074-what-is-the-self-learning-ai-in-homebase-3- (last accessed Oct. 19, 2023).

[25] *Id.*




35. Eufy readily admits that "[t]he Cross-Camera Tracking function depends on a human feature recognition algorithm [sic] that determines the similarity of an individual's appearance in two videos to stitch them together. Even if the face is not visible in the video, videos of similar-looking individuals are still identified and stitched together."[26]

36. In fact, Eufy's data collection and storage systems were recently scrutinized because of their vulnerability. Until recently, Eufy's storage procedures

[26] Eufy, *supra* note 21.

placed Plaintiffs' and Class Members' biometrics at risk in precisely the manner the Illinois Legislature enacted BIPA to prevent.

37. In late 2022, technology reporters and security experts "accused … Eufy of lying to users that their video streams were end-to-end encrypted, even though users were easily able to access the streams using simple browser tools and a desktop media player."[27]

38. As data and technology giant Cisco explains, encryption is "the process of converting or scrambling data and information into an unreadable, encoded version that can only be read with authorized access … and is [a] widely used security tool that can prevent the interception of sensitive data, either while stored in files or while in transit across networks."[28]

39. The reporters' accusations turned out to be correct. "In a series of emails … Anker [] finally admitted its Eufy security cameras [were] *not* natively end-to-end encrypted—they [could] and *did* produce unencrypted video streams from Eufy's web portal."[29]

40. In fact, Eufy's systems were so vulnerable that, despite "a Eufy Support representative['s] state[ment] that [facial] thumbnails [were] restricted by account logins[,]"[30] one security expert was easily able to hack into his own Eufy system—

---

[27] Kyle Barr, *Eufy Finally Admits its "Local" Cameras Were Sending Unencrypted Streams, Claims It Will Do Better*, Gizmodo (Feb. 1, 2023) *available* https://gizmodo.com/eufy-local-security-camera-cloud-unencrypted-scandal-1850059207 (last accessed Oct. 23, 2023).

[28] Cisco, *What is Encryption?* available https://www.cisco.com/c/en/us/products/security/encryption-explained.html (last accessed Oct. 23, 2023).

[29] Sean Hollister, *Anker Finally Comes Clean About Its Eufy Security Cameras*, The Verge (Jan. 31, 2023) *available* https://www.theverge.com/23573362/anker-eufy-security-camera-answers-encryption (Oct. 23, 2023) (Emphasis in original).

[30] Kevin Purdy, *Eufy's "No Clouds" Cameras Upload Facial Thumbnails to AWS*, ARS Technica (Nov. 30, 2022) *available* https://arstechnica.com/gadgets/2022/11/eufys-no-clouds-cameras-upload-facial-thumbnails-to-aws/ (last accessed Oct. 23, 2023).

despite unplugging it—and "could pull up a thumbnail image of himself, an image of the feed shortly before he was visible, and—perhaps more concerning—ID numbers indicating his recognized face and his status as the camera owner."[31]

41. And, although Eufy has since hired "outside security and penetration testing companies to audit [its] practices,"[32] as referenced above, unsecured biometrics stored on easily compromised systems—as Eufy did—is precisely the type of risk BIPA was enacted to protect the subject of a recording from.

42. Indeed, the Illinois Legislature was motivated to enact BIPA to protect unauthorized disclosure of biometrics because "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). Accordingly, because "[b]iometrics [] are biologically unique to the individual [,] once compromised, the individual has no recourse, is at heightened risk for identify theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

43. Due to these concerns, BIPA provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual's biometrics unless it informs that person in writing that biometric identifiers or information will be collected or stored. *See* 740 ILCS 14/15(b).

44. Likewise, BIPA also requires that entities collecting biometrics publish and make publicly available written retention schedules and guidelines for permanently destroying biometrics collected. *See* 740 ILCS 14/15(c).

## II. Illinois' Biometric Information Privacy Act

45. BIPA defines biometric identifiers as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

[31] *Id.*

[32] Sean Hollister, *supra* note 29.

46. Similarly, BIPA defines biometric information as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

47. Facial geometry is a permanent, unique biometric identifier associated only with a specific person. Collecting and storing a person's face geometry exposes them to serious and irreversible privacy risks. For example, if a device or database containing stored images of facial geometry is hacked, breached, or otherwise compromised, the person has no means by which they can prevent identity theft or unauthorized hacking of secure devices which use facial recognition to grant access.

48. Recognizing the need to protect citizens from these risks, Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") in 2008, to regulate companies that collect and store biometric information, such as facial geometry. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276.

49. Accordingly, BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers and/or biometric information unless it first:

1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;

2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

740 ILCS 14/15(b).

50. Additionally, Section 15(a) requires that entities in possession of biometrics publish a schedule detailing its retention and destruction plans concerning the biometric information in its possession.

51. Section 15(a) of BIPA provides that:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

52. As alleged below, Defendant's practices of collecting, storing, and using delivery drivers' biometric identifiers and biometric information without informed written consent violated all three prongs of § 15(b) of BIPA. Furthermore, Defendant violates § 15(a) of BIPA by failing to publish and make publicly available any written policy regarding Defendant's schedule and guidelines for retaining and permanently destroying individuals' biometrics.

## III. Defendant Violates Illinois' Biometric Information Privacy Act

53. Unbeknownst to Plaintiffs, and in direct violation of § 15(b)(1) of BIPA, Defendant collected, scanned, and then indefinitely stored in an electronic database Plaintiffs' biometric information and biometric identifiers when Plaintiffs and Class Members made deliveries to the homes of Defendant's customers who used Defendant's security system. Each time Plaintiffs and Class Members made a delivery to Defendant's customers' homes, Defendant's cameras collected Plaintiffs' face and/or hand geometry and stored the images of Plaintiffs' face and body geometry in an electronic database without ever informing Plaintiffs in writing that it was doing so.

54. Moreover, in direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Defendant never informed Plaintiffs and Class Members who had their biometric information and biometric identifiers collected, of the specific purpose and length of time for which their biometrics would be collected, stored, and used, nor did Defendant ever obtain a written release.

55. Finally, and in direct violation of § 15(a) of BIPA, Defendant failed to publish policies for public access identifying its retention schedules or guidelines for permanently destroying any of these biometrics.

## CLASS ALLEGATIONS

56. Plaintiffs bring this matter on behalf of themselves and all similarly situated in the following class:

> **Illinois Class:** All natural persons in Illinois who are delivery drivers and who, when making deliveries, had their biometric information and biometric identifiers collected, stored, and scanned by Eufy cameras and software from November 27, 2018, to present.

57. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendant's counsel.

58. The members of the Class are so numerous that joinder of all members is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, such information can be ascertained through appropriate discovery from records maintained by Defendant and its agents.

59. Plaintiffs reserve the right to expand, limit, modify, or amend the class definition, including the addition of one or more Subclasses, in connection with their motion for class certification, or at any other time, based on, *inter alia*, changing circumstances and new facts obtained.

60. **Numerosity:** Class Members are so numerous that joinder of all members is impracticable. Plaintiffs believe that there are thousands of delivery drivers who are Class Members described above who have been damaged by Defendant's unlawful collecting, storing, and using of their biometric identifiers and biometric information.

61. **Commonality and Predominance:** The questions of law and fact common to the class which predominate over any questions which may affect individual class members include, but are not limited to:

a. whether Defendant collected or otherwise obtained Plaintiffs' and the Class's biometric identifiers and/or biometric information;

b. whether Defendant properly informed Plaintiffs and the Class that it collected, used, and stored their biometric identifiers and/or biometric information;

c. whether Defendant obtained a written release (as defined by 740 ILCS 14/10) to collect, use, and store Plaintiffs' and the Class's biometric identifiers and/or biometric information;

d. whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, whichever comes first;

e. whether Defendant used Plaintiffs' and the Class's biometric identifiers and/or biometric information to identify them;

f. whether Defendant destroyed Plaintiffs' and the Class's biometric identifiers and/or biometric information once that information was no longer needed for the purpose for which it was originally collected; and

g. whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

62. **Typicality:** The claims of the named Plaintiffs are typical of the claims of the Class because the named Plaintiffs, like other members of the Class, made deliveries to customer's homes and had their biometric information and biometric identifiers collected, stored, and analyzed by Defendant's cameras and software without providing consent, nor did Defendant provide Plaintiffs and Class Members with written policy made publicly available establishing a schedule and procedure for permanently destroying Plaintiffs' and Class Members' biometric information and identifiers.

63. **Adequate Representation:** Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Neither Plaintiffs, nor their counsel, have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs are able to fairly and adequately represent the interests of the Class. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this complaint to include additional Class Representatives to represent the Class or additional claims as may be appropriate.

64. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Class is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent, or contradictory judgments, and would magnify

the delay and expense to all parties and to the court system resulting in multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents fewer management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

**COUNT I**
**Violation of 740 ILCS 14/15(b)**
**(On Behalf of Plaintiffs and the Class)**

65. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

66. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or information. . ." 740 ILCS 14/15(b).

67. Defendant failed to comply with these BIPA mandates.

68. Fantasia Trading LLC is a limited liability company doing business as Eufy and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

69. Plaintiffs and Class Members are delivery drivers in Illinois who had their "biometric identifiers" and "biometric information," including scans of face and hand geometry, collected, captured, received, or otherwise obtained by Eufy from video and/or images recorded by a Eufy device and scanned by Eufy software to

differentiate between humans and non-human entrants on the camera-owner's property.

70. Plaintiffs and Class Member's face, body, and hand geometry was uploaded, stored, and mechanically measured to create numerical representations used as "face templates" that can be used to uniquely identify Plaintiffs and Class Members. *See* 740 ILCS 14/10.

71. Eufy systematically and automatically collected, captured, or otherwise obtained Plaintiffs' and Class Members' "biometric identifiers" (which it used to create and store uniquely identifying face geometry) without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them.

72. Plaintiffs' and the Class's scans of face and/or hand geometry can and are used to identify them and, therefore constitute "biometric identifiers" and/or "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

73. Defendant never informed Plaintiffs or members of the Class in writing that their biometric identifiers and/or biometric information were being collected, captured, stored, and/or used, nor did Defendant inform Plaintiffs and members of the Class in writing of the length of time for which their biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

74. By collecting, capturing, storing, and/or using Plaintiffs' and members of the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiffs' and the Class's right to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

75. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interest of Plaintiffs and the Class by requiring Eufy comply with BIPA's requirements for the collection, storage, and use of "biometric information" and "biometric identifiers" as

described herein; (3) statutory damages of $1,000.00 pursuant to 740 ILCS 14/20 for each negligent violation of BIPA committed by Eufy; (4) statutory damages of $5,000.00 pursuant to 740 ILCS 14/20 for each intentional or reckless violation of BIPA committed by Eufy; and (5) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

**COUNT II**
**Violation of 740 ILCS 14/15(a)**
**(On Behalf of Plaintiffs and the Class)**

76. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

77. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention and deletion policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

78. Defendant failed to comply with these BIPA mandates.

79. Defendant is a limited liability company and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

80. Plaintiffs are individuals who had their "biometric identifiers" and "biometric information" captured and/or collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

81. Plaintiffs' biometrics could be used to identify them and, therefore, constituted "biometric identifiers" and "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

82. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying Plaintiffs' biometric identifiers and information as specified by BIPA. *See* 740 ILCS 14/15(a).

83. Because Defendant lacked retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometrics, the only reasonable conclusion is that Defendant has not, and will not, destroy Plaintiffs' and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied.

84. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA's requirements for the collecting, storing, and using biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgement against Defendants as follows:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel of the Class;

B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*, with respect to Plaintiffs and Class Members;

C. Awarding statutory damages to Plaintiffs and Class Members of $1,000.00 pursuant to 740 ILCS 14/20(1) for each violation of BIPA

committed negligently, and $5,000.00 pursuant to 740 ILCS 14/20(2) for each violation of BIPA committed intentionally or recklessly;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and members of the Class, including *inter alia*, an order requiring Defendant to collect, store, and use biometric identifiers or biometric information in compliance with BIPA;

E. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees pursuant to BIPA;

F. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable;

G. Awarding Plaintiffs and the Class such other and further relief as equity and justice may require.

**JURY TRIAL DEMANDED**

Under Federal Rule of Civil Procedure 38, Plaintiffs, individually and on behalf of the members of the Class, exercise their right under the Seventh Amendment to the United States Constitution and demand a trial by jury.

Dated: November 27, 2023

Respectfully submitted,

**BURSOR & FISHER, P.A.**

By: /s/ *L. Timothy Fisher*
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
Stefan Bogdanovich (State Bar No. 324525)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
sbogdanovich@bursor.com

*Attorneys for Plaintiffs*